Woodforest Acceptance Solutions

CyberSource Gateway

Executive Summary

CyberSource Gateway is WAS's primary enterprise payment gateway, delivering secure, API-first processing for digital and omnichannel commerce. As a Visa-owned platform, it provides enterprise-grade authorization, tokenization, fraud, and recurring payment capabilities, while WAS remains the acquirer of record—managing onboarding, underwriting, settlement, funding, and risk. In the WAS ecosystem, CyberSource serves as the gateway backbone, enabling merchants, ISVs, and platforms to accept card-not-present and multi-channel payments without owning or maintaining gateway infrastructure.

Strategic Role in the WAS Portfolio

CyberSource is positioned as WAS's default enterprise gateway, providing a unified, long-term foundation for eCommerce, embedded payments, and omnichannel growth—without the inconsistency of supporting multiple third-party gateways.

This strategy enables WAS to:

- Retain full control of the acquiring relationship
- Reduce gateway sprawl and recertification complexity
- Support SMB → enterprise growth on a single gateway stack
- Provide consistent tokenization, fraud tooling, and reporting across channels

Who It's Built For

- ISVs and software platforms embedding payments
- eCommerce and digital-first merchants
- Subscription and recurring-revenue businesses
- B2B and invoice-driven organizations
- Mid-market and enterprise-oriented businesses

Core Use Cases

- Embedded & Platform Payments
- Scalable eCommerce & Omnichannel Acceptance
- Subscription & Stored Credential Models
- Advanced Fraud & Risk Management

Platform Differentiation

Unlike SMB-focused gateways, CyberSource is enterprise-grade by design. It is API-driven, globally scalable, and built on Visa infrastructure (Visa Platform Connect), making it suitable for high-growth, high-complexity environments.

Partner & Merchant Value

For merchants and platforms, CyberSource delivers a future-proof gateway that won't need to be replaced as complexity increases. For partners, it provides a consistent, scalable solution backed by Visa and supported end-to-end by WAS.

For merchants and platforms, CyberSource delivers a future-proof gateway that won't need to be replaced as complexity increases. For partners, it provides a consistent, scalable solution backed by Visa and supported end-to-end by WAS.

---

1. Product Overview

What the Product Is

CyberSource Gateway is a Visa-owned, enterprise-grade payment gateway positioned by WAS as its primary solution for secure and scalable payment processing. It enables merchants and software platforms to accept card-not-present and omnichannel payments through a single, API-first gateway, while WAS remains the acquirer of record—handling onboarding, underwriting, settlement, funding, and risk. This model delivers consistent, enterprise-ready payment capabilities without requiring partners to build, manage, or maintain gateway infrastructure.

Portfolio Strategy

CyberSource Gateway is positioned as the foundational gateway layer in the WAS portfolio for all non-proprietary payment acceptance. By standardizing on a single, Visa-owned enterprise gateway, WAS avoids gateway sprawl while focusing on what it owns best—the acquiring relationship, including onboarding, settlement, funding, and risk. As the default gateway for eCommerce, embedded software, and omnichannel use cases, CyberSource provides a consistent, scalable foundation that enables partners to sell confidently across SMB, mid-market, and enterprise channels as the strategic gateway backbone of the WAS ecosystem.

Ideal Customer Profile (ICP)

CyberSource Gateway works best for merchants and software platforms that need a secure, flexible, gateway-led payment solution without building or maintaining gateway infrastructure themselves. The simple qualifying question is:

"Does this merchant or platform need to accept and manage card-not-present or omnichannel payments across one or more channels using a single, scalable gateway?"

If yes, CyberSource Gateway is very likely a strong fit.

Ideal Customer Segments

- ISVs & Software Platforms
  - Vertical SaaS providers embedding payments into their software
  - Platforms requiring API-first payment acceptance, tokenization, and scalable onboarding
- eCommerce & Digital-First Merchants
  - Direct-to-consumer (DTC) brands
  - Online retailers and marketplaces
  - Subscription-based and recurring billing businesses
- Omnichannel Merchants
  - Merchants selling across online, mobile, and virtual channels
  - Businesses needing consistent payment processing and reporting across channels
- Mid-Market & Enterprise-Oriented Businesses
  - Merchants requiring advanced gateway controls, fraud tools, and reporting
  - Businesses planning to scale locations, merchants, or transaction volume over time

Typical Characteristics

- Primarily card-not-present payment flows (eCommerce, in-app, MOTO, recurring)
- Need for gateway flexibility without POS or hardware dependency
- Preference for WAS-managed onboarding, acquiring, settlement, and funding
- Strong emphasis on security, tokenization, fraud management, and long-term scalability

Vertical-by-Vertical Breakdown

ISVs & Embedded Software Platforms

Pain Points: Software platforms want to embed payments but don't want to build, certify, and maintain direct network or gateway integrations. Gateway switching, re-certification, and merchant onboarding complexity slow growth.

CyberSource Gateway Solves: CyberSource offers API-first, enterprise-grade gateway capabilities for embedded payments, while WAS manages merchant onboarding, compliance, acquiring, and settlement. This allows ISVs to scale payments across merchants and verticals without owning gateway infrastructure.

Opening Line: "If payments are part of your software roadmap, do you really want to own a gateway—or would you rather embed one that's already enterprise-ready?"

Retail (eCommerce & Omnichannel Retailers)

Pain Points: Retailers struggle with fragmented online payment tools, limited fraud controls, and inconsistent reporting across eCommerce, mobile, and virtual sales channels. Many gateways can authorize payments but lack enterprise-grade scalability, tokenization, and risk controls as transaction volumes grow.

CyberSource Gateway Solves: CyberSource provides a single, secure gateway for card-not-present and omnichannel retail transactions, with built-in tokenization, advanced fraud tools, and centralized reporting. When sold by WAS, merchants gain a unified gateway experience while WAS manages onboarding, acquiring, settlement, and funding—removing complexity and operational risk.

Opening Line: "Many retailers outgrow basic eCommerce gateways once volume increases—how are you handling fraud, tokens, and reporting as your online sales scale?"

Subscription & Recurring Billing Businesses

Pain Points: Recurring merchants face failed payments, expired cards, and high churn caused by weak card-on-file management. Basic gateways lack lifecycle tools to support retries, updates, and stored credential best practices.

CyberSource Gateway Solves: CyberSource supports vaulted tokens, recurring billing flows, and account updater services through a single gateway. WAS enables these capabilities while maintaining control over merchant setup, risk, and funding—helping merchants stabilize recurring revenue without custom gateway development.

Opening Line: "How much revenue do you lose each month due to expired cards or failed recurring payments—and what tools are you using today to prevent that?"

B2B & Professional Services

Pain Points: B2B merchants rely on manual invoicing, phone payments, and disconnected virtual terminals, creating reconciliation challenges and delayed payments. Many gateways are built for retail checkout—not B2B payment workflows.

CyberSource Gateway Solves: CyberSource supports virtual terminal, invoicing, Pay-By-Link, and flexible payment flows through a single gateway. WAS wraps these gateway capabilities with acquiring, settlement, and funding support—allowing B2B merchants to modernize payments without replacing upstream systems.

Opening Line: “Are you still taking B2B payments by invoice and phone, or do you have a gateway that supports modern, card-not-present workflows?”

Marketplaces & Multi-Merchant Platforms

Pain Points: Marketplaces struggle with managing payments across many merchants, maintaining token security, and supporting different use cases on a single gateway. Many gateway solutions don’t scale cleanly across multiple merchant accounts.

CyberSource Gateway Solves: CyberSource supports multi-merchant gateway models with tokenization and centralized control, while WAS governs merchant onboarding, underwriting, and settlement. This structure allows platforms to scale safely without becoming a payments company themselves.

Opening Line: “How are you managing payments across multiple merchants today—and who owns the risk and complexity behind the scenes?”

Healthcare, Utilities & Regulated Services

Pain Points: Regulated industries need secure payment acceptance with strict data handling, tokenization, and compliance requirements. Basic gateways often fall short on enterprise security expectations.

CyberSource Gateway Solves: As a Visa-owned gateway, CyberSource delivers enterprise-grade security, tokenization, and fraud controls suitable for regulated environments. WAS strengthens this by managing merchant compliance, risk, and settlement within an acquiring-first model.

Opening Line: “In regulated environments, payments can’t be an afterthought—what gateway are you using to ensure security and compliance at scale?”

NOT a good fit

- Full-Service Restaurants or POS-Heavy In-Store Operations
    - Businesses that require table management, servers, kitchen workflows, reservations, or deep in-store operational features. CyberSource is a gateway—not a POS.

- Merchants Needing POS-Level Inventory or Store Operation.
    - Businesses looking for real-time inventory, staff management, or operational tooling tightly coupled to payments.

- Enterprises With Proprietary Payment Stacks
    - Large national retailers operating custom gateways or direct network integrations that do not align with a standardized gateway model.

- Merchants Seeking Turnkey Hardware or Terminals
    - Businesses expecting a plug-and-play terminal or all-in-one in-store solution without software integration.

- Very Small, Low-Volume Merchants
    - Merchants that only need basic checkout and do not require advanced gateway features like tokenization, fraud tooling, or scalability.

Primary Use Cases

Use Case #1

Problem: We want to embed payments into our software, but building and maintaining a gateway—or managing compliance and merchant onboarding—is too complex and risky.

Feature: CyberSource offers API-first gateway capabilities designed for embedded use cases, while WAS handles merchant onboarding, underwriting, compliance, settlement, and funding.

Value: ISVs and platforms can monetize payments, scale across merchants, and deliver a seamless in-app payment experience—without becoming a payments company themselves.

Use Case #2

Problem: We rely on subscriptions or repeat payments, but failed transactions from expired cards and retries are driving churn and revenue loss.

Feature: CyberSource supports vaulted tokens, stored credential frameworks, recurring billing flows, and account updater services—all managed through a single payment gateway.

Value: Merchants reduce failed payments, improve retention, and stabilize recurring revenue without building custom payment logic or managing sensitive card data.

Use Case #3

Problem: B2B payments are slow and manual—customers pay by phone or invoice, reconciliation is time-consuming, and cash flow is inconsistent.

Feature: CyberSource enables virtual terminal, pay-by-link, and invoicing payment flows through the same secure gateway used for online payments.

Value: Merchants get paid faster, reduce manual handling, and consolidate B2B and digital payments into one reporting and settlement experience powered by WAS.

Use Case #4

Problem: Our online sales are growing, but our current gateway can't keep up—fraud is increasing, approvals are inconsistent, and reporting is fragmented as volume scales.

Feature: CyberSource provides an enterprise-grade payment gateway with advanced fraud and risk tools, tokenization, and Visa-backed routing optimized for card-not-present transactions.

Value: Merchants gain higher approval rates, stronger fraud protection, and a scalable gateway foundation that supports growth—while WAS manages acquiring, settlement, and funding behind the scenes.

High-Level Functionality

CyberSource Gateway enables businesses and software platforms to securely accept, route, and manage digital payments across eCommerce, in-app, virtual terminal, invoicing, and recurring use cases through a single, enterprise-grade gateway. Positioned as WAS's primary gateway offering, it serves as the core payment processing layer for card-not-present transactions, providing authorization, capture, refunds, tokenization, fraud and risk controls, and centralized reporting without requiring merchants or partners to manage direct network or gateway integrations. When sold by WAS, CyberSource is paired with WAS-managed merchant onboarding, acquiring, settlement, and funding—allowing partners and merchants to deliver flexible, scalable payment experiences while WAS handles the operational, compliance, and risk complexity behind the scenes.

Positioning Statement / Elevator Pitch

Short "Walk-up" Pitch (15 Seconds)

"CyberSource is WAS's primary payment gateway for digital and omnichannel commerce. It gives merchants and platforms a Visa-backed, enterprise-grade gateway for secure online, in-app, recurring, and virtual payments—while WAS handles onboarding, acquiring, settlement, and funding."

Competitive Displacement Pitch (Authorize.net/NMI)

"Authorize.Net and NMI work well for basic checkout, but most merchants and platforms outgrow them once volume, fraud, or complexity increases.
CyberSource delivers enterprise-grade gateway capabilities—tokenization, advanced fraud tooling, and scalability—built on Visa's infrastructure. When paired with WAS, merchants get a future-proof gateway without managing multiple providers, re-certifications, or operational lift."

Discovery-Led Opening (Conversation Starter)

"Quick question—are you comfortable with your current gateway as volume scales, or are you starting to see limits around fraud, reporting, or multi-channel payments?"
"That's where CyberSource fits. It's built for growth, not just basic checkout."

Margin Protection / Cost Recovery Pitch

"One hidden cost merchants face isn't pricing—it's failed payments and fraud losses.
CyberSource helps protect margins through stronger authorization performance, fraud controls, and tokenized card-on-file payments that reduce declines. Combined with WAS-managed acquiring and settlement, merchants keep more approved revenue with fewer operational headaches."

Vertical Use-Case Pitch

"Whether you're an eCommerce merchant, subscription business, B2B operator, or software platform, CyberSource adapts.
It supports online checkout, recurring billing, invoicing, virtual terminal, and embedded payments through one gateway—while WAS manages the complexity behind the scenes so payments don't slow growth."

Objection Responses

"I already have a gateway."	That's common—most merchants do. The real question is whether your current gateway will still work as volume, fraud exposure, or complexity increases. CyberSource is built for scale and longevity, with enterprise-grade security and Visa-backed infrastructure, while WAS manages onboarding, acquiring, and settlement.
"Switching gateways sounds painful."	That's a valid concern. CyberSource is API-first and migration-friendly, and WAS handles the onboarding, certification, and transition process. Most merchants switch because the stability and long-term ease outweigh the short-term change.
"My current gateway works fine."	Many gateways work fine—until they don't. The issue isn't today's transactions, it's whether your gateway will support growth, recurring billing, fraud management, and omnichannel expansion tomorrow. CyberSource is designed to grow with the business, not be replaced later.
"I don't have high volume—we're not enterprise."	CyberSource isn't about size—it's about where you're going. Many merchants adopt it before volume spikes so they don't have to re-platform later. You get enterprise-grade capabilities now without outgrowing your gateway later.
"I don't want to manage fraud tools or compliance."	You don't have to. CyberSource provides built-in fraud, tokenization, and security tools at the gateway level, and WAS manages merchant compliance, risk, and settlement. That means more protection with less day-to-day effort from the merchant.
"I don't want to deal with multiple vendors."	That's exactly why WAS pairs CyberSource with its acquiring platform. Instead of juggling a gateway, processor, and support partners, merchants work with WAS as the single point of accountability—while CyberSource runs as the underlying gateway engine.
"We only need something simple right now."	That makes sense—but switching gateways later is far harder than starting with the right one. CyberSource can support simple checkout today while giving you tokenization, recurring billing, and fraud protection when you need them—without another migration.

Key Differentiators

Comparison	CyberSource	Authorize.net	NMI
Fees			
Monthly Software Fee	$20.00	$15.00	$15.00
Extra Features = Extra Monthly	Add on $	Add on $	Add on $
Hardware Ranges	PAX Terminals	X	Varies
Customized Pricing Available	✓	✓	✓
Industry Specific Software			
Business Size	SMB → Enterprise	SMB	SMB → Mid-Market
Gateway Type	Enterprise / API-First	SMB / Legacy	Mid-Market / ISO
Software Type	Cloud/SaaS	Cloud/SaaS	Cloud/SaaS
Merchant Services	In House	In House	In House
Features			
Hosted Checkout Pages	✓	✓	✓
API-First REST Payments	✓	X	✓
Card-Not-Present Processing	✓	✓	✓
Omnichannel Token Reuse	✓	X	✓
Network Tokenization	✓	X	Add on $
Token Vault (Multi-Channel)	✓	✓ (Limited)	✓
Stored Credentials Framework	✓	✓	✓
Recurring / Subscription Billing	✓	✓	✓
Account Updater	✓	Add on $	Add on $
Fraud Filters (Basic)	✓	✓	✓
Advanced Fraud Management	Add on $	X	Add on $
Payer Authentication (3DS)	Add on $	X	Add on $
ACH / eCheck	✓	✓	✓
Virtual Terminal (MOTO)	✓	✓	✓
Pay-By-Link / Invoicing	✓	✓	✓
Marketplace / Multi-Merchant	✓	X	✓
Split / Platform Token Strategy	✓	X	✓
Webhooks / Event Notifications	✓	X	✓
Real-Time Reporting APIs	✓	✓ (Limited)	✓
Settlement & Funding Reporting	✓	X	X
Multi-Currency Support	✓	X	Add on $
International Acceptance	✓	X	Add on $
Enterprise Uptime / SLA	✓	X	Limited
White-Labeling (Gateway UI)	✓	X	Add on $

Key Configurations and Sales Channels

Key Configurations

CyberSource is an API-first, cloud-based payment gateway configured to support card-not-present and omnichannel payment use cases such as eCommerce checkout, in-app payments, virtual terminal (MOTO), invoicing, pay-by-link, and recurring billing. Configuration is based on merchant or platform needs and can include tokenization, stored credentials, fraud and risk tools, payer authentication (3DS), ACH/eCheck, and reporting access. When sold by WAS, CyberSource is provisioned within WAS's acquiring framework, with gateway features enabled based on the merchant's business model, risk profile, and channel requirements—without relying on merchant-managed network integrations.

Sales Channels

CyberSource Gateway is sold through WAS internal sales teams and approved ISO, ISV, and platform partner channels. WAS centrally manages merchant onboarding, gateway provisioning, acquiring setup, certification, settlement, funding, and ongoing support, providing partners with a single point of accountability. This model allows partners to sell an enterprise-grade gateway solution confidently while WAS handles the operational, compliance, and risk complexity behind the scenes.

---

2. Product Capabilities

Feature	Available	Description
Card payment processing	✓	Core gateway APIs support secure card transaction processing end-to-end.
Credit & Debit Card Acceptance	✓	Processes credit/debit card payments through CyberSource gateway services.
Visa Platform Connect (VPC) Processing	✓	Routes eligible transactions over Visa-backed infrastructure for scale and resilience.
API-first REST design	✓	CyberSource Payments is delivered through RESTful APIs designed for modern integrations.
Hosted Checkout	Add on $	Hosted payment pages reduce PCI scope and speed deployment.
Embedded Checkout	Add on $	Secure payment fields embedded directly into the merchant or ISV experience.
Tokenization (TMS)	✓	Replaces card data with secure tokens managed by CyberSource and enabled by WAS.
Network Tokenization	Add on $	Uses Visa and network tokens to improve approvals and reduce card lifecycle issues.
Stored Credentials	✓	Securely stores payment credentials for repeat or future transactions.
Recurring & Subscription Billing	✓	Supports automated, scheduled recurring payments through the gateway.
Account Updater	Add on $	Automatically refreshes expired or reissued card details to reduce declines.
Fraud Management Essentials	Add on $	Entry-level fraud protection powered by Visa data and machine learning.
Decision Manager	Add on $	Enterprise-grade fraud rules, scoring, and optimization for higher-risk merchants.
Payer Authentication (3DS)	Add on $	Optional 3D Secure authentication for higher-risk or regulated transactions.
Virtual Terminal (MOTO)	✓	Enables keyed card payments through a secure web-based interface.
E-Invoicing	✓	Sends digital invoices with integrated payment options.
Pay-By-Link	✓	Accepts payments through secure, shareable payment links.
ACH / eCheck Payments	Add on $	Supports bank-to-bank payments as an alternative to cards.
Multi-Merchant / Platform Support	✓	Designed for ISVs and platforms onboarding multiple merchants with WAS.
Marketplace / Split Payment Flows	✓	Supports platform-level payment structures when configured through WAS.
Webhooks & Event Notifications	Add on $	Provides real-time transaction and payment event updates.
Transaction-Level Reporting	✓	Detailed transaction visibility through CyberSource and WAS reporting tools.
Settlement & Funding Reporting	✓	Clear visibility into batches, settlements, and funding managed by WAS.
Chargeback & Retrieval Reporting	✓	Centralized chargeback and retrieval visibility with WAS support paths.
CSV / Data Export	✓	Exports transaction and reporting data for reconciliation and analysis.
Role-Based Access & Hierarchy Reporting	✓	Merchant- and partner-level reporting views based on WAS permissions.
Global Scalability	✓	Supports growth in volume, merchants, and platforms without re-platforming.
Acceptance Devices (In-Person)	✓	Take in person payments through certified devices offered by WAS.
Standard reports	✓	Core Business Center reports are typically enabled during onboarding for faster reporting access under WAS provisioning.
Custom report builder	✓	Business Center supports custom reports built from standard report “building blocks.
Advanced Reporting	Add on $	Advanced analytics and reporting for additional add on features

Limitations

- No merchant-managed app marketplace or plug-and-play add-ons
- No merchant-facing low-code or drag-and-drop checkout builder
- APIs are not intended for direct merchant customization without WAS involvement
- No native POS, inventory, or employee management functionality
- No ecommerce storefront hosting or website builder
- Limited native consumer UX tools (no catalog, order management UI, or CRM)
- BNPL options are not universally available and are not guaranteed
- Advanced features are modular and not included by default
- Configuration changes are not fully self-service and require WAS enablement
- Reporting UI is operational and not optimized for small-merchant simplicity
- No built-in customer discovery, marketing, or loyalty tools
- Not vertically opinionated; industry-specific workflows require external systems
- Card brand behavior varies for certain features (e.g., descriptors, token usage)
- ACH and alternative payment methods are not enabled by default

User Personas

CyberSource is designed for role-based, operational access rather than employee-level workflows. User access is typically managed through CyberSource Business Center and WAS-defined permissions, supporting technical, financial, and risk-focused users rather than front-line staff. The platform is best suited for organizations that separate payment operations, development, finance, and risk management into distinct roles.

Types of Businesses That Benefit Most

- ISVs and Embedded Payments Platform
  - (Platforms that need scalable, multi-merchant payment acceptance without building an acquiring stack)
- Mid-Market to Enterprise eCommerce Businesses
  - (Merchants with custom or headless checkout experiences requiring API control)
- B2B and Invoice-Driven Businesses
  - (Organizations using pay-by-link, invoicing, stored credentials, and recurring billing)
- Marketplaces and Facilitator-Style Models
  - (Businesses supporting multiple sellers or sub-merchants under a single platform model)

- Omnichannel Businesses
  - (Merchants combining ecommerce, MOTO, invoicing, and alternative acceptance methods through one gateway)

- Businesses With Dedicated Finance and Risk Teams
  - (Organizations that value advanced reporting, reconciliation, fraud controls, and compliance over simplicity)

- Partners Requiring Bank-Sponsored Acquiring
  - (Businesses that need WAS's underwriting, settlement, and regulatory oversight rather than standalone gateway services)

---

3. Architecture & Technical Summary

High-Level Architecture Diagram

CyberSource, when sold and provisioned through Woodforest Acceptance Solutions (WAS), follows a gateway-centric, cloud-native architecture designed for scale, security, and partner enablement. The solution sits between the merchant's checkout experience (eCommerce site, app, invoicing tool, or platform UI) and the card networks, handling payment authorization, fraud decisioning, tokenization, and reporting entirely in the cloud. Merchant or platform systems connect to CyberSource via secure APIs or Unified Checkout, while WAS operates as the acquirer of record, managing merchant onboarding, underwriting, settlement, and funding. Sensitive card data never touches merchant systems; instead, payment information is captured securely and vaulted within CyberSource's infrastructure, reducing PCI scope and operational risk. This architecture enables real-time transaction processing, centralized reporting and risk controls, high availability, and global scalability—allowing merchants, ISVs, and platforms to grow without deploying or maintaining payment infrastructure themselves.

Ecosystem Fit

CyberSource serves as Woodforest Acceptance Solutions' primary enterprise payment gateway, acting as the foundational gateway layer for all digital, embedded, and omnichannel payment acceptance across the WAS ecosystem. CyberSource powers card-not-present transactions for eCommerce, in-app payments, invoicing, virtual terminal, and platform use cases, while WAS owns and manages the acquiring relationship—including onboarding, underwriting, settlement, and funding. By standardizing on CyberSource as the core gateway backbone, WAS enables merchants, ISVs, and partners to scale securely on Visa-aligned infrastructure (VPC) without building or maintaining gateway, network, or compliance complexity themselves.

System Requirements

- Internet-connected environment for real-time transaction processing and reporting
- Modern web browser for access to CyberSource Business Center
- Ecommerce site, mobile app, invoicing system, or platform to originate transaction
- API or Unified Checkout integration implemented by a developer, ISV, or platform
- No on-premise servers or local payment infrastructure required
- PCI-compliant setup with reduced scope due to secure card data capture and vaulting
- WAS-provisioned merchant account for onboarding, underwriting, settlement, and funding
- External POS, ERP, billing, or marketplace systems integrated separately (not included)

Certified Platform

- VPC - Visa Platform Connect

Security & Compliance Summary

- Cloud-native, highly available payment infrastructure operated by Visa/CyberSource
- Secure card data capture with tokenization so sensitive data never touches merchant systems
- PCI DSS compliant payment processing environment with reduced merchant PCI scope
- Network-level security and encryption aligned with Visa standards
- Support for point-to-point encryption (P2PE) and end-to-end encryption where applicable
- Secure API authentication using keys, signatures, and role-based access controls
- Centralized fraud and risk controls through Visa-backed fraud services (e.g., Decision Manager)
- Continuous monitoring, logging, and threat detection across the platform
- Built-in redundancy and disaster recovery to support high uptime and resiliency
- Bank-sponsored acquiring model with regulatory oversight managed by Woodforest Acceptance Solutions

4. Product Configuration & Options

Customizable Settings

- User Roles & Permissions
    - Role-based access controlled through CyberSource Business Center and WAS provisioning.
    - Permissions can be customized by function (finance, risk, operations, developer) and scoped by merchant or portfolio where applicable.

- Fraud & Risk Controls (Decision Manager)
    - Configurable fraud profiles, rules, scoring thresholds, and velocity checks.
    - Ability to tune acceptance, review, or reject logic based on transaction attributes and risk tolerance.

- Payment Methods & Acceptance Rules
    - Enable or disable specific payment methods (cards, ACH, wallets, alternative payments) per merchant.
    - Control transaction types such as auth-only, capture, refunds, partial captures, and voids.

- Tokenization & Credential Management
    - Configuration for stored credentials, network tokens, and customer/payment instrument token usage.
    - Ability to manage credential lifecycle behaviors such as reuse, updates, and expiration handling.

- Payer Authentication (3DS) Settings
    - Configurable authentication flows, thresholds, and exemptions when 3DS is enabled.
    - Ability to apply authentication selectively based on transaction risk or region.

- Checkout Experience (Unified Checkout)
    - Customizable checkout appearance including layout, fonts, and branding elements.
    - Ability to add or remove supported payment methods via configuration rather than code changes.

- Invoicing & Pay-By-Link Settings
    - Custom invoice templates and payment link behaviors where invoicing is enabled.
    - Control over expiration, reuse, and transaction handling settings.

- Reporting & Data Access
    - Report selection and access by user role (transaction, batch, funding, fraud, invoicing).
    - Export format options (CSV, downloadable reports, on-demand reporting).

- Webhooks & Event Notifications
    - Selectable event types and products for webhook subscriptions.
    - Configurable security options including message-level encryption and signature verification.

- Merchant Descriptors
    - Configuration of static or dynamic descriptors where supported by card brand and issuer.

- Operational Controls via WAS
    - Settlement, funding options, and feature enablement governed and configured by Woodforest Acceptance Solutions rather than merchant self-service.

Optional Modules

- Unified Checkout (hosted or embedded checkout experience)
- Network Tokenization
- Account Updater
- Decision Manager (Advanced Fraud Management)
- Fraud Management Essentials
- Payer Authentication (3DS)
- ACH / eCheck Payments
- Webhooks & Event Notifications
- Reporting APIs
- Advanced / Specialized Reporting (fraud, invoicing, tax, subscription reports)
- Dynamic or Custom Merchant Descriptors
- Early or Accelerated Funding (subject to WAS approval)

Hardware Options

- PAX A77 (Acceptance Device)
- PAX A920 Pro (Acceptance Device)

3rd Party Integration Options

- **eCommerce Platforms**
    - (e.g., Adobe Commerce / Magento, BigCommerce, WooCommerce, OpenCart, PrestaShop, Shopify – via certified connectors or ISVs)

- **ERP & Accounting Systems**
    - (e.g., NetSuite, SAP, Oracle, QuickBooks integrations via partners)

- **Risk, Fraud & Identity Providers**
    - (e.g., Riskified, Signifyd, Chargeback management platforms)

- **Vertical-Specific Software**
    - (Hospitality, ticketing, education, healthcare, and B2B systems through certified partners)

- **Custom / Proprietary Platforms**
    - (ISVs and enterprise systems integrating directly via CyberSource APIs)

---

5. Operational Processes

Transaction Methods

- Card-not-present transactions (eCommerce, in-app, digital payments)
- Keyed transactions via virtual terminal (MOTO)
- E-invoicing payments (customer-keyed via invoice or payment link)
- Recurring and subscription transactions
- Pay-by-Link transactions
- Authorization-only transactions (delayed capture)
- Auth + capture (sale transactions)
- ACH / eCheck transactions (when enabled)
- Platform / multi-merchant transactions (ISV or marketplace models)

Reporting Overview

CyberSource Reports

All reports can be filtered to show specific date periods, store locations, users, products, transaction statuses, etc.)

Report Types	Description of Report
Transaction Request	View detailed, transaction-level activity including authorizations, captures, refunds, and voids.
Payment Batch Detail	Review daily batch submissions showing which transactions were sent for settlement and their status.
Payment Batch Summary	Summarized batch totals by currency and payment method for high-level reconciliation.
Payment Events	Track processor payment notifications, status changes, and transaction exceptions.
Transaction Exception Detail	Identify errors and exceptions related to failed or incomplete transactions and follow-on actions.
Processor Events Detail	View processor-level events that impact transaction processing and settlement.
Settlement Details	See settlement activity tied to batches and processor settlement cycles.
Funding Detail	Track funding amounts, dates, and deposits related to merchant settlement activity.
Invoice Summary	Review invoicing activity, billing periods, and invoice totals when invoicing is enabled.
Subscription Detail	View recurring and subscription payment activity and transaction outcomes.
Account Updater Detail	See card updates performed through Account Updater services.
Payer Authentication Detail	Review 3DS authentication results and transaction-level outcomes.
Payer Authentication Summary	Summarized reporting for payer authentication activity and success rates.
Decision Manager Detail	Analyze fraud decisioning results for screened transactions.
Profile Performance Comparison	Compare fraud profile performance to evaluate effectiveness and false-positive impact.
Tax Detail	View tax amounts applied to transactions when tax services are enabled.

Elevate Reporting is also available. See the Payments 101 section for further details and what reports can be generated.

Operational Constraints

Constraints vary by software tier and enabled features.